

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-200196

(43)Date of publication of application : 31.07.1997

(51)Int.Cl. H04L 9/18
G09C 1/00
H04L 9/34

(21)Application number : 08-010105

(71)Applicant : BROTHER IND LTD

(22)Date of filing : 24.01.1996

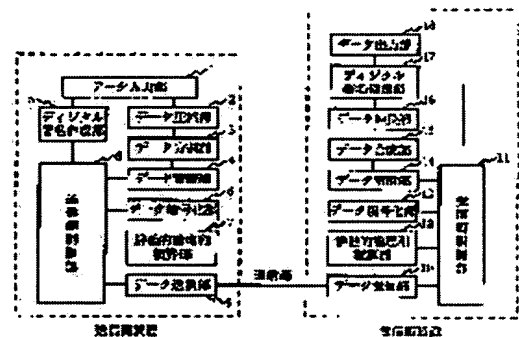
(72)Inventor : NAKAMURA MICHIIHIRO

(54) CIPHERING COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To attain high speed processing by applying ciphering processing to only 1st division data and applying exclusive OR arithmetic operation to 2nd to final n-th division data.

SOLUTION: Data given to a transmitter are given to a data compression section 2, in Which compression processing is conducted and compressed data are divided for 128-bit each by a data division section 3, in which n-sets of division data are generated and stored in a data storage section 4. Then only 1st division data among the division data are subject to ciphering processing at a data ciphering section 6 by using a public key of a recipient (b) and the remaining division data are calculated by an exclusive OR arithmetic section 7 and then the division data are generated and the data are sent by a data transmission section 9 with a digital signature. A data decoding section 13 of a receiver side decodes the 1st division transmission data by using a secret key of a recipient (b) and the 1st division data are decoded and the remaining division transmission data are calculated by an exclusive OR arithmetic section 12 and the division data are decoded.



LEGAL STATUS

[Date of request for examination]

18.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-200196

(43) 公開日 平成9年(1997)7月31日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/18			H04L 9/00	651
G09C 1/00	610	7259-5J	G09C 1/00	610 D
H04L 9/34			H04L 9/00	681

審査請求 未請求 請求項の数 6 O L (全8頁)

(21) 出願番号 特願平8-10105

(22) 出願日 平成8年(1996)1月24日

(71) 出願人 000005267

ブラザー工業株式会社

愛知県名古屋市長区瑞穂区苗代町15番1号

(72) 発明者 中村 道弘

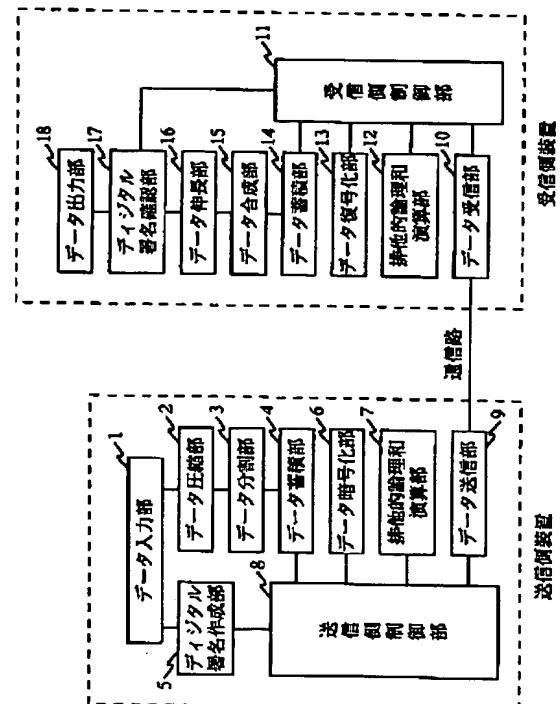
名古屋市長区瑞穂区苗代町15番1号ブラザー工業株式会社内

(54) 【発明の名称】 暗号通信方式

(57) 【要約】

【課題】 通信データ本文全体を暗号化処理する場合よりも短い時間で通信処理を完了することができる暗号通信方式を提供することである。

【解決手段】 送信側では、通信データ本文全体を特定のビット毎にn個に分割し、その第1分割データを暗号化処理して送信データとすると共に、第1分割データと第2分割データとの組から最後の第n-1分割データと第n分割データとの組まで順次排他的論理和を計算して第2分割データから第n分割データまでの送信データを求め、それ等全ての送信データを受信側に送信する一方、受信側では、受信した第1分割送信データを復号処理して元の第1分割データを求めると共に、受信した第2分割送信データから第n分割データについては前記各組毎に排他的論理和を計算して元の第2分割データから第n分割データまでを求め、これ等求められた全ての分割データを合成して元の通信データに復元する。



【特許請求の範囲】

【請求項 1】 通信データを送信側で暗号化して受信側に送信するようにした暗号通信方式において、前記送信側では、

通信データの全体を特定のビット長さ毎に n ($2 \leq n$) 個に分割して、その分割された第 1 分割データと第 2 分割データとの組の排他的論理和を計算して第 2 分割データの送信データを求め、以降、同様にして第 $n-1$ 分割データと第 n 分割データとの組まで順次排他的論理和を計算して第 n 分割データまでの各送信データを求める一方、前記第 1 分割データを暗号化処理して送信可能な暗号化データとし、その暗号化された第 1 分割送信データ及び前記排他的論理和演算された第 2 分割送信データから第 n 分割送信データまでの各送信データを前記受信側に送信し、

前記受信側では、

前記送信側から送信された各通信データを受信して、前記暗号化された第 1 分割送信データを復号処理して元の第 1 分割データを求めると共に、前記第 2 分割送信データと前記復号した第 1 分割データとの組の排他的論理和を計算して元の第 2 分割データを求め、以降、同様にして第 n 分割送信データと復元した第 $n-1$ 分割データとの組まで順次排他的論理和を計算して元の第 n 分割データまで求めた後、前記第 1 分割データから第 n 分割データまでを合成して元の通信データを復元することを特徴とする暗号通信方式。

【請求項 2】 通信データを送信側で暗号化して受信側に送信するようにした暗号通信方式において、

前記送信側では、

通信データの全体を特定のビット長さ毎に n ($3 \leq n$) 個に分割して、その分割された途中の第 i 分割データ

($2 \leq i \leq n-1$) と第 $i+1$ 分割データとの組の排他的論理和を計算して第 $i+1$ 分割データの送信データを求め、以降、同様にして第 $n-1$ 分割データと第 n 分割データとの組まで順次排他的論理和を計算して第 n 分割データまでの各送信データを求める一方、第 1 分割データから前記第 i 分割データまでの各分割データを暗号化処理して送信可能な各暗号化データとし、その暗号化された第 1 分割送信データから第 i 分割送信データまでの各送信データ及び前記排他的論理和演算された第 $i+1$ 分割送信データから第 n 分割送信データまでの各送信データを前記受信側に送信し、

前記受信側では、

前記送信側から送信された各通信データを受信して、前記暗号化された第 1 分割送信データから第 i 分割送信データまでの各送信データを復号処理して元の第 1 分割データから第 i 分割データまでの各分割データを求めると共に、前記第 $i+1$ 分割送信データと前記復号した第 i 分割データとの組の排他的論理和を計算して元の第 $i+1$ 分割データを求め、以降、同様にして第 n 分割送信デ

ータと復元した第 $n-1$ 分割データとの組まで順次排他的論理和を計算して元の第 n 分割データまで求めた後、前記第 1 分割データから第 n 分割データまでを合成して元の通信データを復元することを特徴とする暗号通信方式。

【請求項 3】 前記送信側では、通信データを分割する前にその通信データの圧縮処理を行なうと共に、その圧縮通信データを分割して分割データとし、前記受信側では、前記分割データを合成して元の圧縮通信データを求め、その圧縮通信データを伸長処理して元の通信データに復元することを特徴とする請求項 1 または 2 に記載の暗号通信方式。

【請求項 4】 前記暗号化処理は公開鍵暗号方式を用いたことを特徴とする請求項 1 乃至 3 のいずれかに記載の暗号通信方式。

【請求項 5】 前記暗号化処理は慣用鍵暗号方式を用いたことを特徴とする請求項 1 乃至 3 のいずれかに記載の暗号通信方式。

【請求項 6】 前記送信側では、通信データの全体を特定の長さに圧縮するハッシュ処理を行なうと共に、送信者のデジタル署名を作成して前記受信側に送信し、前記受信側では、復元された通信データの全体についてハッシュ処理を行なうと共に、受信した送信者のデジタル署名を復号し、前記各ハッシュ処理の結果が一致すれば、通信データ及び送信者が正当であるとして処理することを特徴とする請求項 1 及至 5 のいずれかに記載の暗号通信方式。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】本発明は、暗号化されたデータを送受信する暗号通信方式に係り、特に、送信するデータの一部分のみを暗号化することによってデータ全体を暗号化した場合と同様の機密性を保つことができる暗号通信方式に関するものである。

【 0 0 0 2 】

【従来の技術】近年、通信ネットワークの凄まじい発展によりさまざまなデータがネットワークを介して通信されるようになってきている。これらのネットワークには、ネットワーク上での盗聴、通信データの改ざん、送信者を偽るなりすまし等のセキュリティ上の問題が存在している。このようなネットワーク通信路上のデータのセキュリティ確保のために、暗号化したデータを通信する暗号通信方式が幅広く用いられるようになってきている。

【 0 0 0 3 】

【発明が解決しようとする課題】しかしながら、従来の暗号通信方式では、通信データの本文全体が暗号化処理されていたために、通常の暗号化処理を行なわない通信に比較して通信処理に時間がかかるという問題点があった。

【0004】本発明は、上述した問題点を解決するためになされたものであり、通信データの一部分のみに暗号化処理を行なうことによって、通信データの本文全体を暗号化処理した場合と同等の機密性を維持しつつ、短い時間で通信処理を完了することができる暗号通信方式を提供することを目的とする。

【0005】

【課題を解決するための手段】この目的を達成するために、本発明の請求項1に記載の暗号通信方式は、通信データを送信側で暗号化して受信側に送信するようにした方式を対象として、特に、前記送信側では、通信データの全体を特定のビット長さ毎に n ($2 \leq n$) 個に分割して、その分割された第1分割データと第2分割データとの組の排他的論理和を計算して第2分割データの送信データを求め、以降、同様にして第 $n-1$ 分割データと第 n 分割データとの組まで順次排他的論理和を計算して第 n 分割データまでの各送信データを求める一方、前記第1分割データを暗号化処理して送信可能な暗号化データとし、その暗号化された第1分割送信データ及び前記排他的論理和演算された第2分割送信データから第 n 分割送信データまでの各送信データを前記受信側に送信する。

【0006】そして、前記受信側では、前記送信側から送信された各通信データを受信して、前記暗号化された第1分割送信データを復号処理して元の第1分割データを求めると共に、前記第2分割送信データと前記復号した第1分割データとの組の排他的論理和を計算して元の第2分割データを求め、以降、同様にして第 n 分割送信データと復元した第 $n-1$ 分割データとの組まで順次排他的論理和を計算して元の第 n 分割データまで求めた後、前記第1分割データから第 n 分割データまでを合成して元の通信データを復元する。

【0007】従って、通信データを分割して第1分割データのみを暗号化処理し、第2分割データから第 n 分割データまでを排他的論理和演算を行なうことによって通信データの機密性を保つことができるものである。また、暗号化処理はひとつの分割データのみであり、他の分割データは簡単な排他的論理和のビット演算であるので、高速な処理が可能になる。

【0008】また、請求項2に記載の暗号通信方式は、通信データを送信側で暗号化して受信側に送信するようにした方式を対象として、特に、前記送信側では、通信データの全体を特定のビット長さ毎に n ($3 \leq n$) 個に分割して、その分割された途中の第 i 分割データ ($2 \leq i \leq n-1$) と第 $i+1$ 分割データとの組の排他的論理和を計算して第 $i+1$ 分割データの送信データを求め、以降、同様にして第 $n-1$ 分割データと第 n 分割データとの組まで順次排他的論理和を計算して第 n 分割データまでの各送信データを求める一方、第1分割データから前記第 i 分割データまでの各分割データを暗号化処理し

て送信可能な各暗号化データとし、その暗号化された第1分割送信データから第 i 分割送信データまでの各送信データ及び前記排他的論理和演算された第 $i+1$ 分割送信データから第 n 分割送信データまでの各送信データを前記受信側に送信する。

【0009】そして、前記受信側では、前記送信側から送信された各通信データを受信して、前記暗号化された第1分割送信データから第 i 分割送信データまでの各送信データを復号処理して元の第1分割データから第 i 分割データまでの各分割データを求めると共に、前記第 $i+1$ 分割送信データと前記復号した第 i 分割データとの組の排他的論理和を計算して元の第 $i+1$ 分割データを求め、以降、同様にして第 n 分割送信データと復元した第 $n-1$ 分割データとの組まで順次排他的論理和を計算して元の第 n 分割データまで求めた後、前記第1分割データから第 n 分割データまでを合成して元の通信データを復元する。

【0010】従って、分割した通信データの第1分割データから第 i 分割データを暗号化処理し、第 $i+1$ 分割データから第 n 分割データまでを排他的論理和演算を行なうことによって、通信データの最初の部分が特定のフォーマットにされている場合に一つの分割データの暗号化処理のみでは常に同じ暗号化データになる危険性を避けることができ、通信データの機密性の向上を強化することができるものである。

【0011】また、請求項3に記載の暗号通信方式は、前記送信側では、通信データを分割する前にその通信データの圧縮処理を行ない、その圧縮通信データを分割して分割データとし、前記受信側では、前記分割データを合成して元の圧縮通信データを求め、その圧縮通信データを伸長処理して元の通信データに復元する。従って、通信データ本文全体を圧縮処理することによって、通信データの容量を減らすことができ、通信時間及び通信処理時間を短縮することができるものであり、また、圧縮処理されたデータ自体は、通信データ本文の内容を伸長処理しない限り意味をなさないランダムデータとなっているので、排他的論理和演算処理部分のデータの機密性を暗号化処理を行なったものと同等にすることができるものである。

【0012】また、請求項4に記載の暗号通信方式は、前記暗号化処理として、公開鍵暗号方式を用いている。従って、通信者間で暗号通信を行なう際に事前に暗号鍵を共有しておく必要がなく、通信相手の公開鍵をお互いに持つことで暗号通信を行なうことができるものである。

【0013】また、請求項5に記載の暗号通信方式は、前記暗号化処理として、慣用鍵暗号方式を用いている。従って、公開鍵暗号方式よりも高速に暗号化処理を行なうことができるものである。また、大量の暗号文と平文の組を利用する差分攻撃法や線形攻撃法に対して、1回

の通信に使用される暗号文と平文の組は、1組か数組のごく少ないものである。差分攻撃法や線形攻撃法に必要な数の暗号文と平文の組を入手するには非常に時間がかかるために安全性に優れている。

【0014】さらに、請求項6に記載の暗号通信方式は、前記送信側では、通信データの全体を特定の長さに圧縮するハッシュ処理を行なうと共に、送信者のデジタル署名を作成して前記受信側に送信し、前記受信側では、復元された通信データの全体についてハッシュ処理を行なうと共に、受信した送信者のデジタル署名を復号し、前記各ハッシュ処理の結果が一致すれば、通信データ及び送信者が正当であるとして処理する。従って、通信データの本文のデジタル署名を送信することによって、通信データと送信者とが正当であることを確認することができるものである。

【0015】

【発明の実施の形態】以下に、本発明の暗号通信方式を具体化した実施の形態について図面を参照して説明する。

【0016】図1は、本発明の暗号通信方式を適用した通信装置の構成を示すブロック図である。

【0017】送信側装置は、データ入力部1、データ圧縮部2、データ分割部3、データ蓄積部4、デジタル署名作成部5、データ暗号化部6、排他的論理和演算部7、送信側制御部8及びデータ送信部9から構成される。また、受信側装置は、データ受信部10、受信側制御部11、排他的論理和演算部12、データ復号化部13、データ蓄積部14、データ合成部15、データ伸長部16、デジタル署名確認部17及びデータ出力部18から構成される。

【0018】前記データ入力部1は、コンピュータ上等で作成・編集された文章やデータ等を送信側装置に入力するためのインターフェイスである。

【0019】前記データ圧縮部2は、入力データを特定の圧縮フォーマットに従って圧縮処理を行なうものである。

【0020】前記データ分割部3は、圧縮されたデータを128ビット毎に分割するものであり、n個の分割データ(D1, . . . , Dn)を作成するものであるが、最後の第n分割データ(Dn)は128ビットちょうどでなくても構わない。

【0021】前記データ蓄積部4は、暗号化処理及び排他的論理和演算を行なうために分割データを一時的に蓄積しておくものである。

【0022】前記デジタル署名作成部5は、暗号/復号処理方式に公開鍵暗号方式を使用するものであり、入力されたデータ本文全体にハッシュ処理、即ち、通信データの全体を特定の長さに圧縮する処理を行ない、ハッシュデータ(HD)を作成し、このハッシュデータを次の式

$$HD' = EKEb [DKDa (HD)]$$

のように、送信者aの秘密鍵(KDa)を用いて復号化処理したものを受信者bの公開鍵(KEb)を用いてさらに暗号化処理を行なって、送信者aの認証と送信データの正当性を証明するためのデジタル署名(HD')を作成するものである。ここで、前記EKEbは受信者bの公開鍵(KEb)を用いる暗号化処理、前記DKDaは送信者aの秘密鍵(KDa)を用いる復号化処理である。

【0023】前記データ暗号化部6は、データの暗号/復号処理方式に公開鍵暗号方式を使用するものであり、受信者bの公開鍵(KEb)を用いて

$$D1' = EKEb (D1)$$

のように、第1分割データ(D1)の暗号化処理を行ない、第1分割送信データ(D1')を作成するものである。

【0024】前記排他的論理和演算部7は、第2分割データ(D2)から第n分割データ(Dn)までを、次の式

$$Di' = Di \wedge Di-1 \quad (2 \leq i \leq n)$$

を用いて、排他的論理和演算を行ない、分割送信データ(D2', . . . , Dn')を作成するものである。ここで、 \wedge はビット毎の排他的論理和演算であり、以降の式の \wedge も同様の排他的論理和演算である。

【0025】前記送信側制御部8は、送信側装置全体の制御処理を実行するものであって、暗号通信を行なうための制御、通信手順における諸々の制御を実行するものである。

【0026】前記データ送信部9は、デジタル署名データと共に作成された分割送信データの第1分割送信データ(D1')から第n分割送信データ(Dn')までを順次送信するものである。

【0027】前記データ受信部10は、通信路を介して送信されたデータを受信するものである。

【0028】前記受信側制御部11は、受信側装置全体の制御処理を実行するものであり、暗号通信を行なうための制御、通信手順における諸々の制御を実行するものである。

【0029】データ復号化部13は、データ暗号化部6と同様にデータの暗号/復号処理方式に公開鍵暗号方式を使用するものであり、受信者bの秘密鍵(KDb)を用いて

$$D1 = DKDb (D1')$$

のように、第1分割送信データ(D1')の復号化処理を行ない、第1分割データ(D1)を復号するものである。ここで、前記DKDbは受信者bの秘密鍵(KDb)を用いる復号化処理である。

【0030】前記排他的論理和演算部12は、データ復号化部13で復号された第1分割データ(D1)を初期値として、第2分割送信データ(D2')から第n分割

送信データ (D_n') までを、次の式

$$D_i = D_i' \oplus D_{i-1} \quad (2 \leq i \leq n)$$

を用いて、排他的論理和演算を行ない、分割データ (D_2, \dots, D_n) を復元するものである。

【0031】前記データ蓄積部14は、分割データの合成を行なうために、復元された分割データを一時的に蓄積しておくものである。

【0032】前記データ合成部15は、復元された分割データを元のひとつの圧縮通信データに合成するための処理を行なうものである。

【0033】前記データ伸長部16は、合成された圧縮通信データに伸長処理を施して元の通信データに復元するものである。

【0034】デジタル署名確認部17は、暗号/復号処理方式に公開鍵暗号方式を使用するものであり、データ伸長部16で復元された通信データ本文全体のハッシュ処理を行ない、ハッシュデータ (HD_1) を求め、受信したデジタル署名 (HD') を次の式

$$HD = EKEa [DKDb (HD')]]$$

のように、受信者bの秘密鍵 (KDb) を用いて復号化処理したものを送信者aの公開鍵 (EKa) を用いてさらに暗号化処理を行なって、送信者aが作成したハッシュデータ (HD) を取り出し、二つのハッシュデータ

(HD_1 と HD) の値を照合して一致するか否かを確認し、一致する場合には送信者aの認証と送信データとが正当であることを証明し、一致しない場合には途中でデータが改ざんされたか、送信者aを偽ったなりすましが行なわれたとの判断を行なうものである。ここで、前記 $EKEa$ は送信者aの公開鍵 (EKa) を用いる暗号化処理である。

【0035】前記データ出力部18は、デジタル署名確認部17で送信者aの認証と送信データとが正当であることが証明された場合には復元した通信データを出力し、送信者aの認証と送信データとが正当であることが証明されなかった場合にはエラーメッセージを出力するものである。

【0036】このような構成を有する本実施の形態の通信装置に基づく暗号通信方式の送信手順を図2のフローチャートを用いて説明する。

【0037】なお、送信者aと受信者bの間で通信を開始する前に、送信者aと受信者bとは、お互いの公開鍵 (EKa 、 EKb) を入手しておく必要があるが、公開鍵の入手方法は、どのような方法を用いても構わない。

【0038】まず、送信者aは、受信者bに送りたいデータをコンピュータ上で作成し、データ入力部1のインターフェイスを介して送信装置に入力する (S1)。入力されたデータは、デジタル署名作成部5によってデータ本文全体についてハッシュ処理が施され、ハッシュデータ (HD) が作成される。このハッシュデータは、送信者aの秘密鍵 (KDa) と受信者bの公開鍵

(EKb) とを用いて

$$HD' = EKEb [DKDa (HD)]$$

のように暗号化処理がなされて、デジタル署名 (HD') が作成されるのである (S2)。このデジタル署名は、受信側で送信者aの認証と送信データの正当性を証明するために使用される。

【0039】入力されたデータは、データ圧縮部2によって圧縮処理が施され (S3)、圧縮データが作成される。この圧縮データは、入力データサイズよりも小さなサイズとなり、通信データを縮小することができる。圧縮データは、データ分割部3によって128ビット毎に分割され (S4)、n個の分割データ (D_1, \dots, D_n) が作成され、データ蓄積部4に蓄積される。分割データの内の第1分割データ (D_1) のみがデータ暗号化部6によって、受信者bの公開鍵 (EKb) を用いて $D_1' = EKEb (D_1)$ のように、暗号化処理されて (S5)、第1分割送信データ (D_1') が作成される。残りの分割データは、排他的論理和演算部7によって、

$$D_i' = D_i \oplus D_{i-1} \quad (2 \leq i \leq n)$$

の演算を施されて (S6)、分割送信データ (D_2', \dots, D_n') が作成される。

【0040】作成された分割送信データ (D_1', \dots, D_n') は、デジタル署名 (HD') と共にデータ送信部9によって送信される (S7)。

【0041】次に、本実施の形態の通信装置における暗号通信方式の受信手順を図3のフローチャートを用いて説明する。

【0042】通信路を介して送信者aから送信されたデータは、データ受信部10によって受信され (S11)、第1分割送信データ (D_1') は、データ復号化部13によって、受信者bの秘密鍵 (KDb) を用いて $D_1 = DKDb (D_1')$ のように、復号化処理が施され (S12)、第1分割データ (D_1) が復号される。残りの分割送信データ (D_2', \dots, D_n') は、排他的論理和演算部12によって、

$$D_i = D_i' \oplus D_{i-1} \quad (2 \leq i \leq n)$$

の演算が施されて (S13)、分割データ (D_2, \dots, D_n) がそれぞれ復元される。

【0043】復元された分割データ (D_1, \dots, D_n) は、データ合成部15によって合成されて (S14)、元の圧縮データに復元される。この復元された圧縮データは、データ伸長部16によって伸長処理が施され (S15)、元の通信データに復元される。復元された通信データは、送信側と同じハッシュ処理が施され (S16)、ハッシュデータ (HD_1) が作成される。

【0044】また、受信されたデジタル署名 (HD') は、受信者bの秘密鍵 (KDb) と送信者aの公開鍵 (EKa) を用いて

HD = EKEa [DKDb (HD')]]
 のように復号化処理されて (S17)、送信者 a が作成したハッシュデータ (HD) が取り出される。この二つのハッシュデータ (HD1 と HD) は、デジタル署名確認部 17 によって、値が一致するか否かが調べられ (S18)、一致する場合 (S18: YES) には送信者 a の認証と送信データとが正当であることが証明され、データ出力部 18 によって、復元した通信データが出力される (S19)。一方、一致しない場合 (S18: NO) には、途中でデータが改ざんされたか、送信者 a を偽ったなりすましが行なわれたと判断され、データ出力部 18 によって、エラーメッセージが出力される (S20)。

【0045】本発明は、前記実施の形態に限定されることがなく、その趣旨を逸脱しない範囲内で種々の変更が可能である。

【0046】即ち、前記実施の形態では、送信側において通信データの分割処理の前に圧縮処理を行ない、受信側において圧縮通信データを伸長処理して復元するようにしているが、圧縮せずに平文のまま通信データの分割処理を行なって送信することも可能である。

【0047】また、前記実施の形態では、n 個に分割された分割データの内の最初の一つの分割データのみを暗号化処理して送信データとすると共に、残りの全ての分割データを排他的論理和演算して送信データとしたが、分割数 n より小さい数 (例えば、分割数 20 個の内、最初から連続する 3 個とか 5 個) の複数の分割データを暗号化処理してそれぞれ送信データとし、その暗号化処理する最後の分割データの次の分割データから最後の第 n 分割データまでの各分割データについては、前記実施の形態と同様に排他的論理和を計算してそれぞれ送信データを求め、これ等暗号化処理した各送信データと排他的論理和演算された各送信データとを受信側に送信する一方、受信側では、前記実施の形態と同様に、前記暗号化処理した各送信データを複合処理してそれぞれ元の各分割データを求めると共に、前記排他的論理和演算された各送信データについては排他的論理和演算してそれぞれ元の各分割データを求め、これ等求められた最初の分割データから第 n 分割データまでの全ての分割データを合成して元の通信データに復元するように構成してもよい。

【0048】また、前記実施の形態では、暗号化処理の方式に公開鍵暗号方式を使用したか、慣用鍵暗号方式を使用することも可能である。

【0049】さらに、前記実施の形態では、送信側通信装置と受信側通信装置とを別々に構成しているが、送信側通信装置と受信側通信装置の各々の機能を一つの通信装置で構成することも可能である。

【0050】

【発明の効果】以上説明したことから明かなように、本

発明の請求項 1 に記載の暗号通信方式によれば、通信データを分割して第 1 分割データのみを暗号化処理し、第 2 分割データから最後の第 n 分割データを排他的論理和演算を行なうことによって通信データの機密性を保つことができるものである。また、暗号化処理は一つの分割データのみであり、他の分割データは簡単な排他的論理和のビット演算であるので、高速な処理が可能になり、暗号化処理に専用のハードウェアを用意することなく、ソフトウェアのみで装置を構成することができ、通信装置のコストを低減させることができるものである。

【0051】また、請求項 2 に記載の暗号通信方式によれば、分割した通信データの第 1 分割データから第 i 分割データまでを暗号化処理し、第 i+1 分割データから第 n 分割データを排他的論理和演算を行なうことによって、特に、通信データの最初の部分が特定のフォーマットにされているような場合に、一つの分割データの暗号化処理のみでは常に同じ暗号化データになる危険性を避けることができるものであり、通信データの機密性の向上を強化することができるものである。

【0052】また、請求項 3 に記載の暗号通信方式によれば、通信データの本文全体を圧縮処理することによって、通信データの容量を減らすことができ、通信時間及び通信処理時間を短縮することができるものであり、また、圧縮処理されたデータ自体は、通信データ本文の内容を伸長処理しない限り意味をなさないランダムデータとなっているので、排他的論理和演算処理部分のデータの機密性を暗号化処理を行なったものと同等にすることができるものである。

【0053】また、請求項 4 に記載の暗号通信方式によれば、暗号化処理方式に公開鍵暗号方式を使用することによって、通信者間で暗号通信を行なう際に事前に暗号鍵を共有しておく必要がなく、通信相手の公開鍵をお互いに持つことで暗号通信を行なうことができるものである。

【0054】また、請求項 5 に記載の暗号通信方式によれば、暗号化処理方式に慣用鍵暗号方式を使用することにより、公開鍵暗号方式よりも高速に暗号化処理を行なうことができるものである。また、大量の暗号文と平文の組を利用する差分攻撃法や線形攻撃法に対して、1 回の通信に使用される暗号文と平文の組は、1 組か数組のごく少ないものであるため、差分攻撃法や線形攻撃法に必要な数の暗号文と平文の組を入手するには非常に時間がかかるために安全性に優れたものである。

【0055】また、請求項 6 に記載の暗号通信方式によれば、通信データの本文のデジタル署名を送信することによって、通信データと送信者とが正当であることを確認することができるものである。

【図面の簡単な説明】

【図 1】本発明に係る暗号通信方式を適用した通信装置の構成を示すブロック図である。

【図 2】 暗号通信方式の送信手順を示すフローチャートである。

【図 3】 暗号通信方式の受信手順を示すフローチャートである。

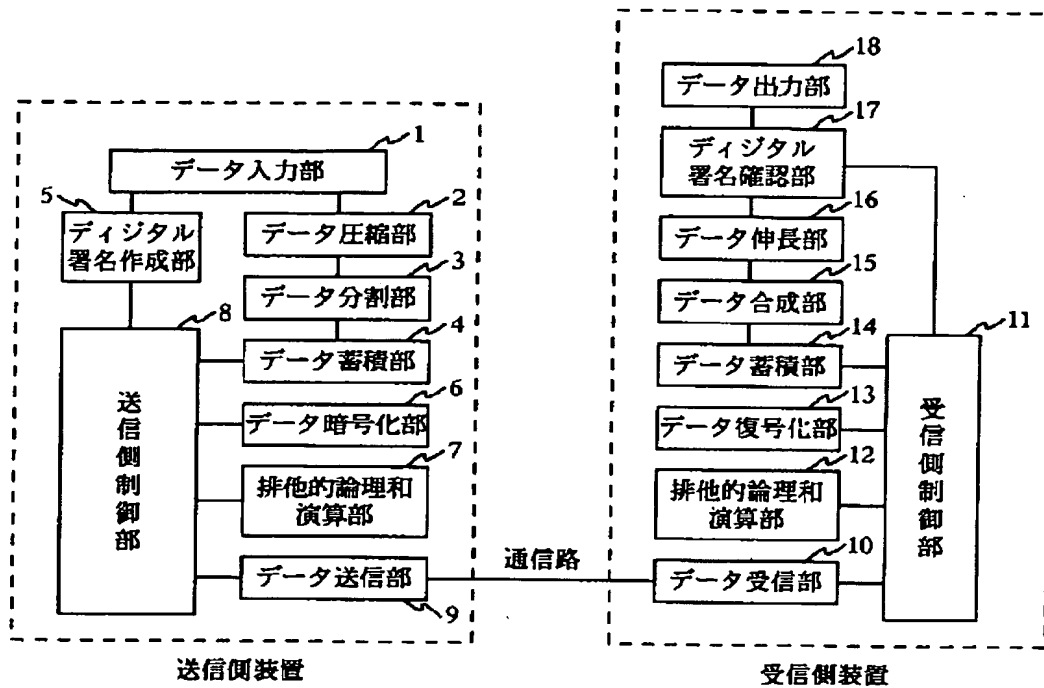
【符号の説明】

- 2 データ圧縮部
- 3 データ分割部
- 5 デジタル署名生成部
- 6 データ暗号化部
- 7 排他的論理和演算部

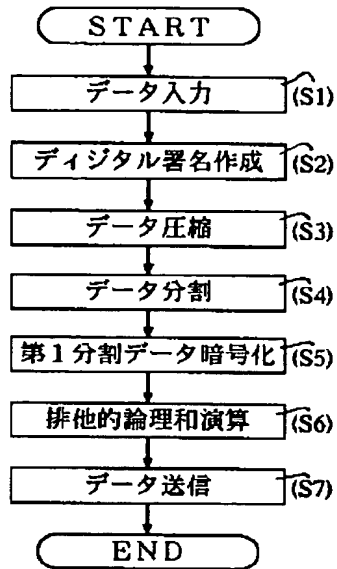
- 8 送信側制御部
- 9 データ送信部
- 10 データ受信部
- 11 受信側制御部
- 12 排他的論理和演算部
- 13 データ復号化部
- 15 データ合成部
- 16 データ伸長部
- 17 デジタル署名確認部
- 18 データ出力部

10

【図 1】



【図 2】



【図 3】

